

Van de Velde

Whistleblowing policy



This policy was approved by the Board of Directors of Van de Velde NV on 27 August 2024.

To all stakeholders

At Van de Velde we do our utmost to exclude any form of misconduct or irregularity within the company. This is covered by the core values of Van de Velde (**'we are authentic'**).



Despite all our efforts, **dangerous, immoral or illegal practices** can still occur.

Everyone who has received information in a work-related context about a breach at Van de Velde can make a report. The reporting procedure is not open only to employees of Van de Velde, but also to other individuals who (have) come into contact with Van de Velde in the course of their duties. The individual reporting such practices, is hereafter called a **"Whistleblower"**.

Within the framework of this policy (hereafter **"Policy"**) **"we"**, **"our"** or **"Van de Velde"** refers to Van de Velde NV with address Lageweg 4, 9260 Schellebelle, Belgium and all direct or indirect daughter entities.

The Management Team is responsible for the implementation of the Policy. Each year the Policy is discussed and reviewed by the Management Team. If necessary, adjustments and improvements are made after approval of the Board of Directors.

This whistleblowing policy protects not only the reporting person but Van de Velde too. Van de Velde collects information that can be useful for eliminating dangerous, immoral and illegal practices. As a consequence, Van de Velde can respond quickly and avoid economic losses.

We ask you to read the Policy, to understand it and to make use of the internal reporting channel before making use of external reporting channels.

If you receive an invitation, please complete our 'Whistleblowing training' on the Van de Velde Academy platform or a classroom training.

If you have any questions or insecurities, please contact the head of the Legal Department of Van de Velde at whistleblowing@vandevelde.eu or by phone on +32 9 365 25 10.

We wish you the very best,

Karel Verlinde, CEO and Herman Van de Velde, chairman Board of Directors





Legal framework



A European Union directive¹ regarding protection for Whistleblowers was adopted in 2019. This directive provides a **high level of protection for persons who report breaches** of certain regulations and matters. The goal of this protection is to encourage the reporting of any breach anyone is aware of.

Under this directive a reporting procedure for Whistleblowers is only mandatory for the following Van de Velde entities:

-  - **Van de Velde NV (Belgium)** whereby the subsidiaries of Van de Velde NV in France and Sweden are covered by the reporting procedure of Van de Velde NV.
-  - **Van de Velde Nederland BV (Netherlands)**

The Policy is in line with the Belgian Law of 28 November 2022 regarding the protection of persons reporting breaches of Union or national law established within a legal entity in the private sector, and with the Dutch Whistleblower Protection Act.

To promote transparency and integrity, Van de Velde has decided to **open the internal report channel to:**

- **alle entities of Van de Velde**
- **alle breaches of internal procedures, codes of conduct and policy documents and any other kind of unethical behavior or professional misconduct**

In this regard, Van de Velde will comply with the applicable privacy laws, including the General Data Protection Regulation and the Belgian Privacy Law.

¹European Union directive 2019/1937 on the protection of persons who report breaches of Union law.

Protection of the Whistleblower



The Whistleblower enjoys protection if it acts in good faith and had reasonable grounds to believe that the reported information about the breach was true at the time of the report.

Besides the Whistleblower, the following persons also receive the same protection:

- Facilitators: persons who assist the Whistleblower during the reporting process (such as trade union officials, colleagues, managers, etc.);
- Third parties connected to the Whistleblower and who could suffer retaliation in a work-related context, such as colleagues or relatives of the Whistleblower;
- Legal entities linked to the Whistleblower in a work-related context or owned by the Whistleblower.

Protection is given in the form of the following measures:

1. Confidentiality

The report manager has sole access to the identity of the reporting person and will keep this secret. The report manager can share confidential information (not including the Whistleblower's personal data) to safeguard feedback towards the Whistleblower.

This confidentiality is also applied to facilitators, third parties who are connected with the reporting person and the legal entities to which the reporting person is linked.

Every effort is made to protect the identity of the persons involved for the duration of the investigation.

2. Possibility of an anonymous report

The reporting person can also opt to report anonymously, in which case the report manager will not know the identity of the reporting person. Persons wishing to report breaches anonymously can do so by filling out the whistleblowing form on the Van de Velde website. The report will be handled without the reporting person receiving any response, as we must not be able to directly or indirectly infer the identity of the reporting person from any report we receive anonymously.

⇒ *In that case we suggest that the reporting person creates an email address that gives no clues as to the reporting person's identity in order to receive a response without compromising the reporting person's anonymity.*

Confidentiality is mutual, which means it also applies to the Whistleblower. Van de Velde expects Whistleblowers to remain silent about their report until they receive a fuller response.

3. Ban on retaliation

Van de Velde undertakes a complete ban on any form of retaliation against the Whistleblower or any other person involved in the matter.

As well as the taking of actual retaliation, threats and attempts to take retaliation are prohibited. Among other things, this means dismissal, bullying and detrimental treatment.

For a full list of banned forms of retaliation see **Annex 1** to this Policy.

What can be reported?



A report under the Policy must be made in the **general interest of Van de Velde**.

Before you make a report under the Policy, we first ask that you use **normal reporting channels** (such as your manager, a confidant or your member of the Management Team). If you do not feel comfortable doing so or are reluctant to make a report through these individuals, you may use this Policy to make a confidential or anonymous report.

The Whistleblower may report **dangerous, immoral or illegal practices**, such as (but not limited to):

1. A crime or violation of a law or regulation or international treaty;
2. A criminal offense, including theft and fraud;
3. A violation of a code of conduct, policy or procedure applicable within Van de Velde such as:
 - a. The Code of Conduct for own workforce;
 - b. The Policy against price fixing;
 - c. The Policy Against Corruption and Bribery;
 - d. The Policy on Insider Trading;
 - e. The Environmental Policy;
 - f. The Ethical and Social Charter;
 - g. The Privacy Policy for own workforce;
 - h. The Privacy policy for consumers;
 - i. The Business Partner Code of Conduct.
4. A breach of privacy and personal data protection, and network and information systems security;

5. Any other kind of unethical behavior or professional misconduct.

These matters may be reported while they are occurring, after they have occurred or if they will occur in the future.

It is requested that the reporting person **always** reports this type of breach (or suspicion of such breaches). Breaches (or suspicion of such breaches) relating to members of the Board of Directors, members of the Management Team or other managers must be reported.

The reporting procedure is not meant for issues affecting individuals, such as a conflict between an employee and the employee's manager. If a report is received about such issue, the report manager will provide information to the reporting person about the person or persons to whom such issues can be addressed.

Who can make a report?

Anyone who has obtained information **in a work-related context** about a breach within Van de Velde can make a report.

The following persons may use the reporting channel (among others):

- Employees
- Former employees
- Members of the Management Team
- Members of the Board of Directors
- Job students
- Trainees (paid or unpaid)
- Job Applicants
- Volunteers
- Contractors, subcontractors and suppliers (and their staff and home workers)
- Consultants
- Agents
- Employers
- Shareholders

If a breach is reported in the area of financial services, products and markets, and in the area of prevention of money laundering and terrorist financing, the reporting person can also enjoy protection if this information was acquired **outside a work-related context**.

What about reports that prove to be untrue?

Report in good faith

The person who reports a breach that is untrue or for which there are no reasonable grounds **in good faith** continues to enjoy protection.

Report in bad faith

The reporting person who **knowingly** reports **false information** does so **in bad faith** and is not protected. In that case, Van de Velde may impose appropriate disciplinary measures, as provided for in the employee handbook and providing false attestations or documents or making false statements, for example, constitutes urgent cause justifying the immediate dismissal of the employee.

Furthermore, the reporting person can commit the crime of slander or libel for which criminal law sets appropriate sanctions. Victims of such reports or public disclosures in bad faith may also claim compensation.

How can I report?

Report your concern over a (suspicion of) breach as soon as possible using one of the following options.



Written and verbal reports with the report manager (Head of Legal)

For reports concerning the Legal Department: Head of HR.

WRITTEN

- Using the [Whistleblowing form](#) on the website of Van de Velde (CAN BE ANONYMOUS)
- By email: whistleblowing@vandevelde.eu

VERBAL

- By phone: +32 (0)9 365 25 10
- Face-to-face meeting:
By appointment via whistleblowing@vandevelde.eu or +32 (0)9 365 25 10
- Without appointment at the report manager's office

Confirmation of the report to the Whistleblower within 7 days of receipt of the report

Start investigation

Feedback by report manager to Whistleblower within reasonable term, no later than 3 months after acknowledgement of receipt of report

Retention of whistleblowing report: identifying data are erased after the report has been handled; the anonymised report itself is retained for 5 years (in accordance with GDPR)

Practical info for reporting

Below we provide additional practical information for submitting a report.

1. Content of the report

In order to investigate a report in detail, we ask that you provide the following information:

- Your contact information to the extent you did not make the report anonymously
- Your relationship with Van de Velde
- Description of the breach
 - o When
 - o What
 - o Where
- Any information about those involved with the breach

We don't ask you to gather evidence, but rather to substantiate the report for a faster procedure.

2. Investigation by the report manager

The report shall be received and handled by the report manager in compliance with the principles of confidentiality, impartiality and fairness to all concerned.

The report manager is the head of the Legal Department. After receiving the report, the report manager will ensure the careful follow-up of the report and an investigation will be conducted.

Persons named in the report or identified during the investigation may be contacted if deemed necessary for the investigation. In this case, confidentiality of the report will always be taken into account. In doing so, the report manager will evaluate whether contacting these individuals may not harm the investigation.

3. Entry in the report register

After the report manager receives the report, the report shall be entered into a report register. If the Whistleblower has made an oral report by telephone or through a face-2-face meeting, an accurate record shall be made of that oral report. This report shall be made available to the Whistleblower so that the Whistleblower can review it, correct it if necessary and sign it before it is included in the report register.

4. External report


It is strongly recommended that you first report violations through Van de Velde's internal reporting channel. This allows Van de Velde to investigate the report and take any appropriate action.

Within the European Union, a Whistleblower has the option of reporting a breach within the scope of relevant legislation externally to a local competent authority responsible for receiving and investigating Whistleblower reports.

The authorities authorized to receive and process an external report can be consulted in **Appendix 2**. The Federal Ombudsman is responsible for referring an external report to the competent authority within Belgium.

Privacy policy

1. General



As stated above, we include certain personal data relating to a report in a **report register**. These personal data are processed by Van de Velde NV as controller and/or by another entity of Van de Velde NV in as far as this is necessary to process the report. We do not use an external service provider.

2. What personal data can we process?

We take due care with the processing of this data in accordance with the applicable privacy legislation, particularly the General Data Protection Regulation and the Belgian Privacy Law. That means that we do not process personal data that is not relevant. If we do, this is erased immediately.

We process the name, position and contact details of the Whistleblower, any other person to whom the protective measures can apply and the persons/entities involved.

We process information about (possible) misconduct of data subjects. The reported information may also include other sensitive categories of personal data, such as information about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union relations, health and sexual relations or sexual orientation. We handle this sensitive personal data in a secure and confidential manner.

3. Who do we share your personal data with?

The report manager only has access to the personal data. The personal data can be handed over to governmental or judicial authorities if legally obligated.

4. Why do we process your personal data?

We will process the personal data for the investigation and follow-up of the report.

In addition, personal data may be processed to comply with reasonable requests from competent bodies and authorities, to hand over as evidence to police or judicial authorities if a crime or illegal act has occurred, or to establish or exercise legal claims.

The legal basis for this processing is:

- legitimate interest of Van de Velde to create a safe, respectful and fair working environment
- legal obligation of Van de Velde to assess and investigate whistleblowing reports

5. How long do we retain your personal data?

The personal data are erased once the report has been handled. The report itself is retained for 5 years in anonymous form.

6. What are your privacy rights?

You have the right to receive information about your personal data processed by us, have your personal data corrected or deleted. To do so, please contact privacy@vandevelde.eu. In the event of a removal request, it may be that the legitimate interests of Van de Velde require further processing of the personal data. We will inform you of this within 30 days.




In case of questions or complaints, please contact privacy@vandevelde.eu. You also have the right to file a complaint with the competent data protection authority.




Annex 1: List of banned retaliation types

This list is non-exhaustive:

- Suspension, temporary standing down, dismissal or similar measures;
- Demotion or denial of promotion;
- Transfer of duties, changing of location of workplace, reduction of pay, changing of working hours;
- Withholding of training;
- Negative performance review or job reference;
- Imposition or application of a disciplinary measure, reprimand or other sanction, such as a financial sanction;
- Coercion, intimidation, bullying or exclusion;
- Discrimination, detrimental or unequal treatment;
- Failure to convert a temporary contract of employment into a permanent open-ended contract of employment, if the employee had the justifiable expectation of being offered open-ended employment;
- Failure to renew or early termination of a temporary contract of employment;
- Damage, including reputational damage, including on social media, or financial disadvantage, including loss of turnover and loss of income;
- Inclusion on a blacklist based on an informal or formal agreement for a whole industry or branch, as a consequence of which the person is unable to find another job in that industry or branch;
- Early termination or notice of termination of a contract for the supply of goods or the provision of services;
- Withdrawal of a licence or permit;
- Psychiatric or medical referral.

Annex 2: Competent authorities (EU)

Country	Competent authorities
Belgium 	<ul style="list-style-type: none"> ➤ The Federal Ombudsman ➤ FPS Economy, SMEs, Middle Classes, and Energy ➤ FPS Finance ➤ FPS Public Health, Food Chain Safety and Environment ➤ FPS Mobility and Transport ➤ FPS Employment, Labour and Social Dialogue ➤ Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid (Federal Public Planning Service for Social Integration, Poverty Control, Social Economy and Large City Policy) ➤ Federaal Agentschap voor Nucleaire controle (Federal Agency for Nuclear Control) ➤ Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (Federal Agency for Medicines and Health Products) ➤ Federaal Agentschap voor de veiligheid van de voedselketen (Federal Agency for the Safety of the Food Chain) ➤ Belgische Mededingingsautoriteit (Belgian Competition Authority) ➤ Gegevensbeschermingsautoriteit (Data Protection Authority) ➤ Autoriteit voor Financiële diensten en Markten (Financial Services and Markets Authority) ➤ Nationale Bank van België (National Bank of Belgium) ➤ College van toezicht op de bedrijfsrevisoren (Belgian Audit Oversight Board) ➤ The authorities stated in article 85 of the law of 18 September 2017 to prevent money laundering and terrorist financing and limiting the use of cash ➤ Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater (National Committee for the security of the supply and distribution of drinking water) ➤ Belgisch Instituut voor postdiensten en telecommunicatie (Belgian Institute for Postal Services and Telecommunications) ➤ Rijksinstituut voor ziekte- en invaliditeitsverzekering (National Institute for Health and Disability Insurance) ➤ Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen (National Institute for Social Security Insurance for the Self-employed) ➤ Rijksdienst voor Arbeidsvoorziening (National Employment Office) ➤ Rijksdienst voor Sociale Zekerheid (National Social Security Office) ➤ Sociale Inlichtingen en Opsporingsdienst (Social Information and Investigation Service) ➤ Autonome dienst Coördinatie Anti-Fraude (CAF) (Autonomous Anti-Fraud Coordination Service) ➤ Scheepvaartcontrole (Shipping Inspectorate)
Netherlands 	<ul style="list-style-type: none"> ➤ Autoriteit Consument en Markt (Netherlands Authority for Consumers and Markets) ➤ Autoriteit Financiële Markten (Netherlands Authority for the Financial Markets) ➤ Autoriteit persoonsgegevens (Dutch Data Protection Authority) ➤ Nederlandse Bank N.V. ➤ Huis (House) ➤ Inspectie gezondheidszorg en jeugd (Health and Youth Care Inspectorate) ➤ Nederlandse Zorgautoriteit (Dutch Healthcare Authority) ➤ Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Authority for Nuclear Safety and Radiation Protection) ➤ appropriate organisations and management bodies that have responsibilities or powers in one of the areas stated in article 2, first paragraph of the Directive
Denmark 	<ul style="list-style-type: none"> ➤ Datatilsynet ➤ Justitsministeriet ➤ Forsvarsministeriet ➤ Eksterne whistleblowerordninger oprettet i medfør af sektorspecifik EU-lovgivning, jf. § 2, opretholdes.

Finland 	<ul style="list-style-type: none"> ➤ Oikeuskanslerinviraston ➤ the Finnish Financial Supervisory Authority (FIN-FSA) ➤ the Tax Administration
Spain 	<ul style="list-style-type: none"> ➤ la Autoridad Independiente de Protección del Informante, A.A.I.
Germany 	<ul style="list-style-type: none"> ➤ die externe Meldestelle des Bundes (beim Bundesamt für Justiz) ➤ externe Meldestellen der Länder ➤ die Bundesanstalt für Finanzdienstleistungsaufsicht ➤ das Bundeskartellamt